February 2023

Automated Initiative Compliance Platform

Eliav Kahan

Mike Lee

Helen Chou McCabe

AUTOMATED INITIATIVE COMPLIANCE PLATFORM

Introduction

Generally, running awareness or promotional initiatives that select users or groups using first party data requires obtaining multiple approvals. For example, a company or other organization may have internal policies relating to such data for which compliance is important. Compliance with such protocols may be important to maintain brand reputation and user trust.

The use of first party data in initiatives is growing and expected to continue to grow, thus improvements to current systems may be desired in order to continue to scale with such growth. Providing users with the ability to monitor and audit the use of first party data in initiatives and automatically detect non-compliant initiatives that do not have the proper approvals may further improve such systems.

Summary

Computer-implemented systems and methods for providing automatic detection of non-compliant initiatives (e.g., promotional or awareness strategies) with the disclosed technology can be accomplished by monitoring initiatives, finding a non-compliant initiative, displaying a non-compliant initiative in a dashboard, sending alerts of the non-compliance to a user, and automatically pausing the non-compliant initiative.

In some instances, a user may be notified of initiatives that are non-compliant within a particular time (e.g., 48 hours) of the initiative becoming non-compliant by viewing a dashboard. Some examples of initiatives that are at risk of being non-compliant are those that use first party data in selecting users for paid media or when audience lists are created with first party data. Such an initiative may be non-compliant, for instance, if the initiative does not have proper

approvals from internal teams, is modified to use first party data, or has approvals removed when the initiative was previously compliant. For example, a user may view a dashboard on a user interface that displays all initiatives that are compliant and non-compliant. In this scenario, a non-compliant initiative may surface to the dashboard and be visible to the user as a non-compliant initiative within a particular time (e.g., 48 hours) of the initiative becoming non-compliant. The user can then see on the dashboard which approvals are missing for a non-compliant initiative to become compliant.

In some instances, a user may receive an alert that an initiative is non-compliant within a particular time of the initiative becoming non-compliant. The system or method may monitor the initiatives and send alerts to users when a non-compliant initiative is detected. For example, the system or method may alert when a non-compliant initiative surfaces on the dashboard within 48 hours of non-compliance. The alerts may be sent to specified users based on the severity of the alert or the user's role. Alerts to the user of non-compliant initiatives may occur at any specified regular interval, such as daily or hourly. For instance, daily alerts may show a user the top non-compliant initiatives.

When an initiative is non-compliant, such as for not having the necessary approvals, the initiative may be automatically paused within a particular time of the dashboard surfacing the non-compliant initiative or a user receiving an alert that the initiative is non-compliant. In another instance, the non-compliant initiative may receive the appropriate approvals within a particular time of the dashboard surfacing the non-compliant initiative or a user receiving an alert of the non-compliance, making the initiative compliant and appearing on the dashboard as compliant instead of non-compliant. The system or method may regularly monitor the dashboard to determine whether an initiative is non-compliant and pause any non-compliant initiatives once

detected. In some instances, an application programming interface (API) may automatically pause the non-compliant initiative within a particular time of it becoming non-compliant. Once an initiative is automatically paused for noncompliance, an alert of this information may be sent to the appropriate owners.

In some instances, the user may be able to identify which conditions trigger noncompliance. For example, a user may specify that an initiative that is using first party data must be approved by an internal policy team in order to be compliant. Thus, the dashboard may display the initiative as non-compliant, or a user may receive an alert that the initiative is non-compliant, within a particular time of the initiative becoming non-compliant if the initiative does not have approvals from the necessary team(s). The user may also be able to sort the dashboard display by a specified criterion, such as by start date, compliance, or approval type.

In some instances, the approvals for initiatives using first party data may be audited by the group launching the initiatives. For example, the system or method may automatically check that the group is approved to run an initiative that uses first party data. Additionally, the system or method may systematically audit existing initiatives, for example by checking for compliance every hour or every day. For instance, an initiative or group of initiatives may be audited for compliance with any of the various approvals that the initiative needs in order to be successfully launched.

In some instances, an API may verify the status of an initiative as being compliant or non-compliant with the various approvals necessary for the initiative. For example, a call to the API may be made to ensure that existing initiatives using first party data are compliant (e.g., an initiative has all required approvals), that they have the approvals required to generate user lists for the initiative, and that they do not proceed until all approvals are obtained. The API may also

automatically pause non-compliant initiatives within a particular time of the initiative becoming non-compliant. Different tools may call the API in order to confirm that initiatives and audiences have the appropriate approvals before proceeding with launching an initiative that uses first party data.

Detailed Description

Figure 1 depicts an example computing system 100 in which systems and methods in accordance with the present disclosure can be executed. The computing system comprises a user computing device 102 containing one or more processors 112, memory 114 which may contain data 116 and instructions 118 configured to carry out the methods disclosed herein, and a user input component 122. The user input component can be, for example, a touch display or physical buttons within the user computing device 102. The computing system 100 further comprises a network 180 and a server computing system 130. The server computing system 130 comprises one or more processors 132, and memory 134 which may contain data 136 and instructions 138 configured to carry out the methods disclosed herein. It should be appreciated that any combination or order of systems and methods disclosed herein can be performed on the user computing device, server computing system, or similar. For example, all processes can be performed on the user computing device 102 or the server computing system 130.

Figure 2 depicts an example embodiment of a dashboard 200 that may display to a user that an initiative is compliant or non-compliant according to the present disclosure. For example, the dashboard 200 may be visible to a user via a user interface on a user computing device 102. The dashboard 200 may use a table to display all initiatives in the rows 216, and columns for each initiative that show a name for the initiative 202, an id number for the initiative 204, the initiative start date 206 and end date 208, whether the initiative is using first party data 210,

whether the initiative is compliant or non-compliant 212, and whether the initiative has obtained the various approvals required 214.

On the dashboard 200, the using first party data 210 and approvals 214 columns may be displayed to a user as a “Yes” or “No,” or as “True” or “False.” The column for using first party data 210 may be “Yes” or “True” if the initiative uses first party data to select audiences for paid media or if audience lists for the initiative were created using first party data. The dashboard 200 may display various types of authorizations or approvals 214 that are required for the initiative, such as approvals from internal policy teams, whether the initiative was modified to use first party data, or whether approvals were removed that made the initiative non-compliant. For example, the dashboard may provide an approvals column 214 for approval by the security group labeled “Security Approved,” an approvals column for approval by the privacy group labeled “Privacy Approved,” and an approvals column for compliance with executive review labeled “Executive Compliant.”

The dashboard 200 may display all initiatives and surface a non-compliant initiative within 48 hours of the initiative becoming non-compliant. Once an initiative surfaces as non-compliant, the total compliance 212 column for the initiative may display “Non-compliant.” A user can then view the dashboard 200, find the initiative by name 202 or id 204, and see which approvals 214 are needed for the initiative to become compliant. Once the approvals for a non-compliant initiative are obtained, the total compliance 212 column for the initiative may display “Compliant” and the initiative can be launched.

Referring now to Figure 3, an example embodiment of an alerting system 300 to notify a user that an initiative is non-compliant according to the present disclosure. An initiative 302 may require several approvals before it can be launched. If the initiative does not have all the

approvals needed, for example if it has only two of the three approvals necessary, then a user 304 may receive an alert that the initiative is non-compliant 306 within 48 hours of the complaint becoming non-compliant. The alert 306 may include information about the initiative, such as the name of the initiative, its id, and which approvals it needs to become compliant. The computing system 100 may monitor all initiatives in order to detect when an initiative is non-compliant and send alerts 306 to users 304 when an initiative is non-compliant. For example, an alert 306 may be sent to a user 304 when a non-compliant initiative surfaces on the dashboard 200. A user 304 may be sent an alert based on the user's role or the severity of the alert. Alerts of non-compliant initiatives 306 may be sent to users 304 at a specified regular interval, for example alerts may be sent daily to some users and hourly to other users. For instance, when alerts of non-compliant initiatives 306 are sent at specified intervals, the alerts may show a user 304 a specified top number of non-compliant initiatives. The alert that an initiative is non-compliant 306 may be a notification on a computing device, an email, or an alert on a smart phone 308.

Figure 4 depicts an example embodiment of automatically pausing an initiative 400 when the initiative is non-compliant according to the present disclosure. The computing system 100 may monitor all initiatives in order to detect when an initiative is non-compliant. When an initiative is detected as non-compliant, the system may automatically pause the initiative. For example, the dashboard may surface a non-compliant initiative 216, then within 48 hours the initiative may be automatically paused 402 to prevent the initiative from launching without the required approvals. In another example, a user 304 may receive an alert that an initiative is non-compliant 306, then within 48 hours the initiative may be automatically paused 402. An application programming interface (API) may automatically pause a non-compliant initiative. For example, the API may be called when a non-compliant initiative is detected, such as when

the dashboard surfaces with a non-compliant initiative 216 or when a user 304 receives an alert that an initiative is non-compliant 306, then the API may automatically pause that initiative 402 within 48 hours of it becoming non-compliant. After an initiative is automatically paused for noncompliance, the appropriate owners of the initiative 404 may be alerted that the initiative is non-compliant 406. The alert 406 may include information about the initiative, such as the name of the initiative, its id, and which approvals it needs to become compliant.

Figures

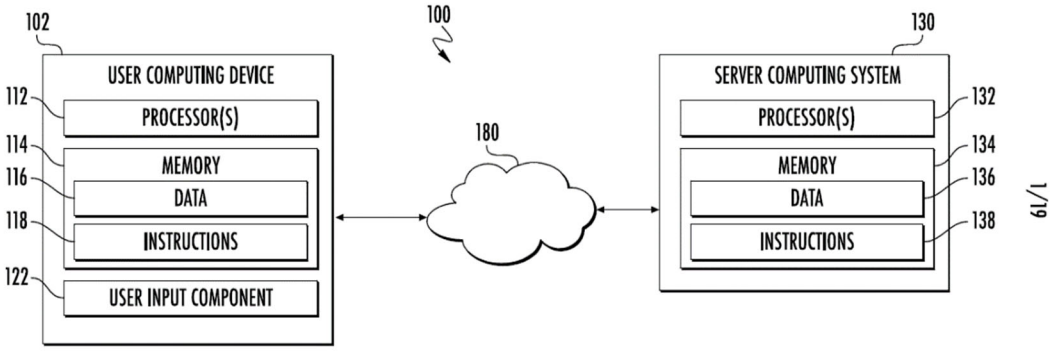

FIG. 1

200

202 Initiative	204 Id	206 Start Date	208 End Date	210 Using First Party Data	212 Total Compliance	Security Approved	Privacy Approved	...	214 X Approved
Initiative 1	12345	2022-01-01	2022-02-01	Yes	Non-compliant	No	Yes	...	No
Initiative 2	67890	2022-01-10	2022-02-10	Yes	Compliant	Yes	Yes	...	Yes
Initiative 3	13579	2022-01-20	2022-03-20	Yes	Non-compliant	Yes	No	...	Yes
...	...	...	...	...	...	...	...	...	...
Initiative N	24680	2022-12-01	2023-01-01	Yes	Non-compliant	No	No	...	No

216

FIG. 2

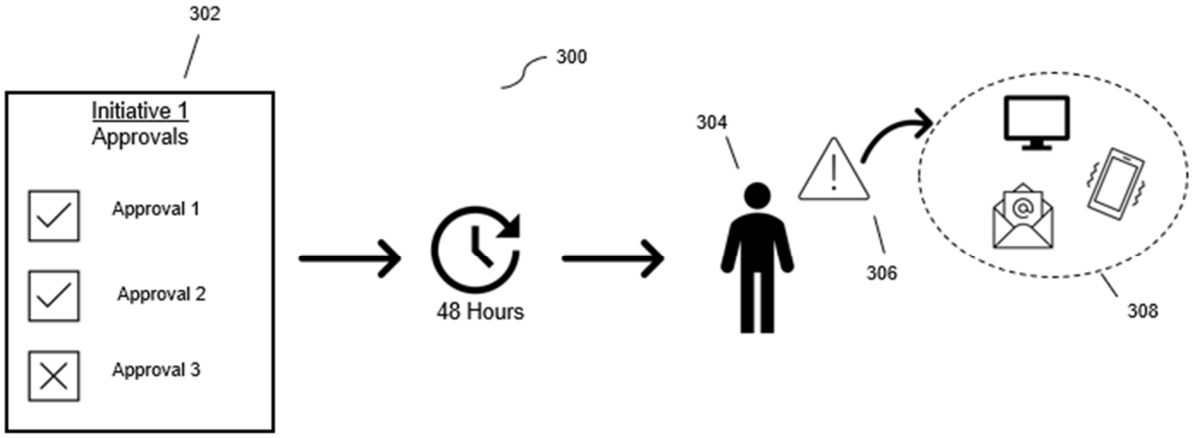

FIG. 3

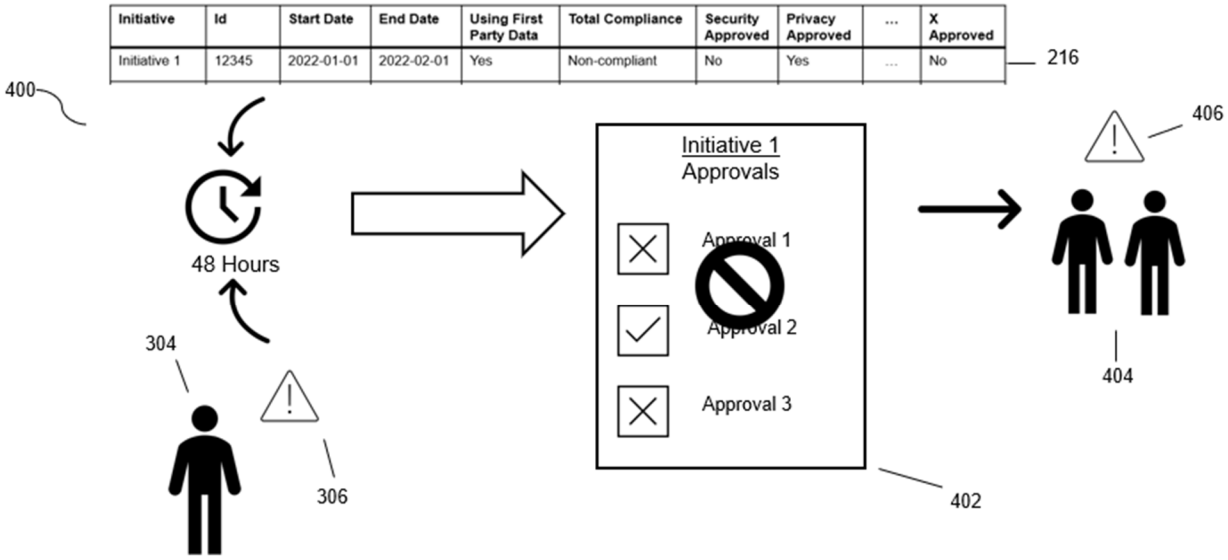

FIG. 4

Abstract

The present disclosure describes computer-implemented systems and methods for automatically detecting non-compliant initiatives by monitoring the system and displaying non-

compliant initiatives in a dashboard that shows a user the approvals that are needed for the initiative to be compliant or alerting a user that the initiative is non-compliant. A non-compliant initiative may then be automatically paused to prevent the non-compliant initiative from launching.